UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,035	12/30/2003	Jaroslaw Sydir	Intel-014PUS	9234

7590 03/28/2007

Daly, Crowley & Mofford, LLP
c/o PortfolioIP
P.O. Box 52050
Minneapolis, MN 55402

EXAMINER	
WILLIAMS, KENT L	
ART UNIT	PAPER NUMBER
2139	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/749,035	**Applicant(s)** SYDIR ET AL.	
	Examiner Kent L. Williams	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 22 February 2007.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 February 2007 and 30 December 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. Objections to the Drawings are withdrawn. Amendments to the drawings have overcome the previous objections to Figures 1, 5 and 6.

Specification

2. Objections to the specification are withdrawn. Amendments to the specification have overcome the previous objections to the specification on page 2.

Claim Objections

3. Objections to the claims are withdrawn. Amendments to claims 21 and 25 have overcome the previous objections.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. (Previously Presented). Claims 1-28, rejected under 35 U.S.C. 103(a) as being unpatentable over Cruikshank (U.S. Patent No. 6,829,315), **has been withdrawn**.

6. (Rejection Maintained, additions underlined). Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cruikshank (U.S. Patent No. 6,829,315) in view of Constant (U.S. Patent No. 4,107,458).

Cruikshank teaches claims 1, 5-12, 18, 21-23 and 25-27 via the use of an alignment buffer for "Alignment of Parallel Data Channels Using Header Detection and Signaling. (Title)." Cruikshank defines his invention as: "...The alignment buffer **225** has a length that is a multiple of a frame length [or a packet] for the (M) bit parallel channels **231**. This buffer length has a wrap-around effect that causes the alignment buffer **225** to write headers at repeating addresses. Repeating header addresses reduce the complexity of the buffer logic. (Column 3, lines 61-67)." Further, "A repeating header address is typically located at the beginning of the memory space and reduces the complexity of the buffer logic. (Column 5, lines 37-39)." Cruikshank explicitly teaches the use of his alignment buffer within a *generic* digital data communications system, which inherently will have a media and switch fabric to send signals across the network and network processors for encoding (synonymous with encrypting and ciphering, Encarta® World English Dictionary) and multiplex control; See

Figure 3. The Examiner wishes to take official notice that a processor will have processing contexts associated therewith (for any given node), and the context will remain associated with the packets, for any one processing schedule, even when stored in a buffering device. Please see the reference given in the "Response to Arguments" below, and column 4, lines 38-47 of Constant (each "context" can be denoted as K_N, where each context of encryption has a particular key, K, and data, S, associated thereto). Figure 3 shows such elements: "media switch fabric" (blocks 302 and 321), "crypto system" (blocks 307 and 324), and alignment buffer (block 325). Cruikshank intends for his alignment buffering system to be versatile in its use, suggesting, "various features described [in Cruickshank's patent] could be combined ... to form multiple variations of the invention. (Column 4, lines 5-10)." The Examiner interprets Cruikshank's disclosure to suggest his invention be used with *any* data communications system, whether or not the system performs clear-text operations or cryptographic/encoding/ciphering operations on the data. Figure 3 teaches the inherent details of such a system, which are expressed within the last 3 blocks: Writing the header data at the beginning of the buffer address space (6th block down) that inherently would write the remaining packet data subsequent to the header, and then transfer the data to the media and switch fabric's buffering system interface for external transfer (using its inherent "interface"); See column 4, lines 45-67 and column 5, lines 1-8 for details. The motivation behind altering the prior-art cryptographic/encoding/ciphering systems is that those systems are "...[then] prevented from detecting false headers in the user data and misaligning the parallel channels.

(Column 1, lines 42-44)." A cryptographic system is otherwise known as cryptographic algorithms programmed within an application specific integrated circuit (ASIC).

Cruikshank teaches claims 2-4, 13-17, 19-20, 24 and 28: As previously stated, Cruikshank's invention is solely based on its versatility as an enhancement for *any* data communications system and *any* interface which it may implement. Again, this is proven as illustrated in Figure 3, block 315 "Optical system," which teaches the use of the SPI4 interface. As well, Cruikshank does not limit his invention to specific optical communication systems, and therefore teaches the use of other systems and also encompassing NPSI interfaces. However, both SPI4 and NPSI define interfaces/protocols for OC-192 signals, which Cruikshank does teach as "The data communications system **350** is configured to operate as follows. The demux **304** receives and processes an OC-192 signal. (Column 4, lines 30-32)." Please see slide 12 of the "Optical Internetworking Forum Report" presentation for further validation. Cruikshank inherently teaches that the end-of-packet transfer would be less than the predetermined size for the protocol used, which is the motivation for his invention: "As a result, the alignment buffer is prevented from detecting false headers in the user data and misaligning the parallel channels. (Column 1, lines 42-44)." This is true despite the byte allocation, which is determined based on the internal/external protocols and algorithms used within the system and not the system per se. The instant application shares the same motivation, stated as, "...the header may not be a multiple of [the predetermined buffer length]... (Page 6, lines 6-7)." It is also inherent that the alignment buffer would transfer the aligned data to the transfer buffers of the media and switch fabric. The exemplary system for embodying Cruikshank's invention directly corresponds to a router given the functions the system, as a whole, performs. It can also be said that his invention could be embodied alongside a router, thereby saying: "it has a router." Cruikshank only implicitly teaches the use of the interface protocols/systems of the instant application. Despite, inclusion of any interface system/protocol (inclusive SPI4 and NPSI) within Cruikshank's invention is the intention, as his invention is conducive to and intended for any interface (as shown above).

Cruikshank teaches the method and apparatus of a versatile alignment buffer for use in *any* data communication system configuration and *any* media and switch fabric interfaces. However, Cruikshank does not ***explicitly*** teach the use of cryptographic processing prior to the alignment buffer.

Constant teaches a general-purpose network processor "Cipher Computer and Cryptographic System. (Title)." Constant describes his invention as: "The general purpose of this invention is to provide small size low cost apparatus for the digital implementation of high capacity high speed stream and block cipher devices. (Column 3, lines 1-5)." Please note that the processing contexts (denoted as 'K'), variable length "mpacket" possibilities (denoted as 'S' and inclusive of 16 bytes) and even more versatility of his invention is described throughout the disclosure, but most notably within lines 33-52 of column 6 and within lines 38-64 of column 4. The versatility of Constant's invention pertinent to the instant application is summarized as "The system of the present invention can be operated as either a fixed or programmable cipher device. (Column 6, lines 33-34)." The Examiner interprets this summary, in conjunction with the rest of the disclosure, to give enablement for his invention to work with hardwired circuits ("crypto units"/ASICs), or by per process programmable device programming to accommodate *any and all* cryptographic algorithm processing. Please note the disclosure of "...a fully programmable block cipher device of the proposed standard [...] and, a fixed (non-programmable) device can be obtained by eliminating the 56 chips needed to implement the ROM **40**. (Column 9, lines 39-46)." In short, Constant's invention is capable of multiple (more than two) versatile block and stream ciphering devices ("crypto units") encompassed as a network processor ("has a router"/"corresponds to a router"): "...applications include and are well suited for the encryption of signals in digital communications networks and the protection of sensitive exchanges between central processors and their terminals, for example in banking, retail point-of-sale, credit verification, personnel files, and medical files, and other applications. (Column 10, lines 22-29)."

It would have been obvious at the time the invention was made to one having ordinary skill in the art to use Constant's invention as intended and include the extra efficiency of Cruikshank's alignment buffer to further enhance the data rate efficiency between the media and switch fabric used at the time the invention was made. Constant teaches a very general-purpose ciphering/encrypting/encoding network processor. Cruikshank teaches a general-purpose alignment buffer and supportive system for use as a data communication system at the time the instant invention was made. It is beneficial to implement Constant's invention (aforementioned) using state-of-the-art means, which is further enhanced using Cruikshanks alignment buffer for use with state-of-the-art data communication systems.

Therefore, it has been shown that, at the time the invention was made, a person having ordinary skill in the art whom is implementing a plurality of modernized cryptographic units of Constant would require the general-purpose alignment buffer of Cuikshank in order to interface with modern-day media and switch fabric transmit buffers (where the only other option is software data realignment). Even further, software data realignment is overlooked because the implementation of "crypto units" (known in the art as "encryption accelerators") would inevitably undo any processing-time savings (acceleration) given by the "crypto units."

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

8. (Previously Presented). Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-29 of copending Application No. 10/749,913. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claimed subject matter of both applications is drawn to a network processor containing crypto units encapsulating cipher cores, processing contexts of the crypto units, buffering mechanisms corresponding to the processing contexts, multiplexer type devices, processing as 16 byte blocks using 64 byte storage allocations, and a network switch and/or router. The following is the claim correspondence from the instant application to the copending application: (cryptographic network processor) claims 1, 5, 7, 8, 9, 18, 21, 23, 25 and 27 to claims 1, 10-12, 18, 20 and 25; (cryptographic processing contexts) claims 6, 10, and 11 to 2, 3, 4, 15, 16, 21, 22, 23, 26, 27 and 28; (byte allocations) claims 15, 16 and 17 to claims 8, 9 and 19; (switch/router and interfaces) claims 2, 3, 4, 12, 13, 14, 19, 20, 24 and 28 to claims 24 and 29.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

9. (Previously Presented). Claims 1-28 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of copending Application No. 10/741,676. Although the conflicting claims are not

identical, they are not patentably distinct from each other because the claimed subject matter of both applications is drawn to a network processor containing crypto units encapsulating cipher cores, processing contexts of the crypto units, buffering mechanisms corresponding to the processing contexts, and a network switch and/or router. The following is the claim correspondence from the instant application to the copending application: (cryptographic network processor) claims 1, 5, 7, 8, 9, 18, 21, 23, 25 and 27 to claims 1, 5, 9, 14 and 18; (cryptographic processing contexts) claims 6, 10, and 11 to 2, 6 and 10; (byte allocations) claims 15, 16 and 17 to claims 3, 7, 11 and 16.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Response to Arguments

10. Applicant's arguments, see lines 13-18 of page 12, filed 22 February 2007, with respect to claims 1-28 have been fully considered and are persuasive. The rejection given under 35 U.S.C. 103(a) as being unpatentable over Cruikshank (U.S. Patent No. 6,829,315) of claims 1-28 has been withdrawn.

11. Applicant's arguments filed 22 February 2007, with respect to the rejection given under 36 U.S.C. 103(a) as being unpatentable over Cruikshank (U.S. Patent No. 6,829,315) in view of Constant (U.S. Patent No. 4,107,458) have been fully considered but they are not persuasive. The arguments presented within the remarks will be addressed in the order given:

[Page 11] The objections to the drawings have been overcome due to the distinction of figure 1 as prior-art and other informality corrections.

[Page 12] The objections to the specification have been overcome due to the minor informality corrections. The objections to the claims have been overcome due to minor informality corrections. Amended claim 1 has overcome the single-reference 35 U.S.C. 103(a) rejection because it now includes the specific symmetric/asymmetric key "crypto system." The single-reference rejection was given on semantic grounds, which is to say that "crypto system," as given in the unamended claims, read on encoding/enciphering/encrypting. However, where "crypto system" is defined as "encrypting data to form ciphered data so that a…cryptographic key may decrypt the ciphered data," "crypto system" no longer reads on the synonymous encoding/enciphering/encrypting. Despite, Constant still teaches such a "crypto system."

[Page 13, ¶1] Referring to the 35 U.S.C. 103(a) rejection supra, Constant teaches a general-purpose system and method for all block-ciphering algorithms inclusive RSA, AES, etcetera, that do use cryptographic keys for encryption and decryption. The allegation that Cuikshank nor Constant disclose or suggest an alignment buffer is incorrect. Cruikshank teaches a general-purpose alignment buffer, and Constant teaches a general-purpose block ciphering cryptographic system. Please note that both of these inventions are *general-purpose*, which is to say they were designed with the intent to be implemented within any system requiring such functionality (and not limited to the embodiments presented within the patents).

[Page 13, ¶2] Cruikshank does not explicitly teach the use of cryptographic processing prior to the alignment buffer because he does not want to limit his invention, rather allowing it to remain a general-purpose. However, the Examiner has found that Cruickshank implicitly teaches a cryptographic processor prior to the alignment buffer, as the source of data is immaterial to the invention: Please note that "decrypting" is a form of "decoding" and Figure 2 of Cruikshank in light of amended claim 1 (regarding "the broadest possible sense [of a decoder]" per page 13, line 13 of the remarks).

[Page 13, ¶3-4] Cruikshank does not limit his invention to a decoder prior to the alignment buffer. Please see Cruikshank, Column 5, lines 60-67. Constant does not limit his invention, nor was such high-speed data communications such a concern during the time of Constant. Please see Constant, Columns 10 and 11, lines 12-68 and 1-7.

[Page 14, ¶1-2] The instant application shares the same motivation as Cruikshank regarding the use of an alignment buffer, stated as, "...the header may not be a multiple of [the predetermined buffer length]... (Page 6, lines 6-7)." Cruikshank states the same as, "The alignment buffer **225** has a length [... that] has a wrap-around effect that causes the alignment buffer **225** to write headers at repeating addresses. Repeating header addresses reduce the complexity of the buffer logic. (Column 3, lines 54-59)." The use of Cruikshanks' alignment buffer is explicitly stated as the same reason given within the instant application. Constant, a general-purpose "encryption accelerator," would necessitate an alignment buffer if it were designed for use on the modern OC-192 interface due to time constraints given by the high-speed data transfers in order to maintain full utilization of the OC-192 system (where software header alignment is not feasible).

[Page 14, ¶3] In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

[Page 14, ¶4-5] The applicant alleges that claims 9, 18, 21 and 25 recite, “the limitation of an alignment buffer connected to a crypto system” within lines 15-16. The Examiner can not determine such a limitation within the claim language of claims 9, 18, 21 and 25. The closest limitation of the instant application, as amended, to the alleged limitation, is: “an alignment buffer to *receive* header data and ciphered data from the crypto system. (Claim 25).” Receiving data from one element by another does not indicate that they are “connected.”

[Page 14, ¶6 and page 15, ¶1] Please see “context switch” from the Free On-Line Dictionary Of Computing (FOLDOC), first paragraph. The “operating system” of the instant invention would be the control given to run multiple “crypto units.”

[Page 15, ¶2] FOLDOC states “Many operating systems implement concurrency by maintaining *separate environments or ‘contexts’* for each process. (¶1).” By definition, each context is a pseudo-environment having its own set of registers and memory space, where each "buffer element" is merely a register.

Conclusion

12. This action is not made final. However, all grounds give this action merit for finality (e.g., no new search was required and/or the original grounds of rejection was maintained).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kent L. Williams whose telephone number is 571-272-1376. The examiner can normally be reached on Mon-Fri 7:00-4:30 with alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kent Williams
12/07/2006

Taghi T. Arani
Primary Examiner.
3/26/07